540, 220

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
5 août 2004 (05.08.2004)

PCT

(10) Numéro de publication internationale
WO 2004/066195 A1

(51) Classification internationale des brevets[7] :
G06K 19/073

(21) Numéro de la demande internationale :
PCT/FR2003/003657

(22) Date de dépôt international :
10 décembre 2003 (10.12.2003)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
0216378 20 décembre 2002 (20.12.2002) FR

(71) Déposant : OBERTHUR CARD SYSTEMS S.A. [FR/FR]; 102, boulevard Malesherbes, F-75017 Paris (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)* : DISCHAMP, Paul [FR/FR]; 26, rue Saint Lambert, F-75015 Paris (FR). GIRAUD, Christophe [FR/FR]; 7, Rue Fustel de Coulanges, F-75005 Paris (FR).

(74) Mandataire : SANTARELLI; 14, avenue de la Grande Armée, B.P. 237, F-75822 Paris Cedex 17 (FR).

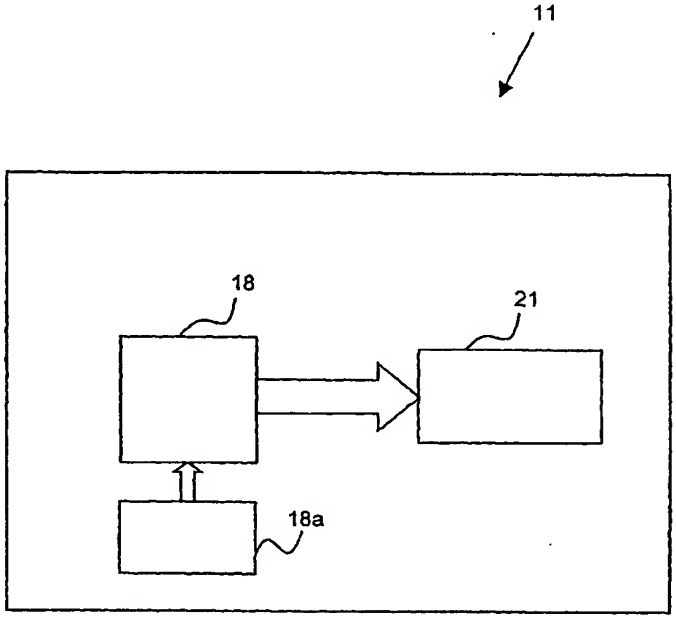
(81) États désignés *(national)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) États désignés *(régional)* : brevet ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet

[Suite sur la page suivante]

(54) Title: SECURE ELECTRONIC ENTITY FOR TIME CERTIFICATION

(54) Titre : ENTITÉ ÉLECTRONIQUE SÉCURISÉE PERMETTANT UNE CERTIFICATION DU TEMPS



(57) Abstract: The invention concerns a secure electronic entity (11) containing a time measuring unit (18) and comprising a unit (21) for certifying an information concerning a date or a time interval, the certifying unit (21) receiving from the time measuring unit (18) data concerning the date or the time interval and producing certification data of the information concerning a date or a time interval addressed to and external entity. The invention is applicable in particular to microcircuit cards.

[Suite sur la page suivante]

WO 2004/066195 A1

eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

Publiée :

— *avec rapport de recherche internationale*

(57) Abrégé : Cette entité électronique sécurisée (11) contient une unité (18) de mesure du temps et comporte une unité (21) de certification d'une donnée relative à une date ou une durée, l'unité (21) de certification recevant de l'unité (18) de mesure du temps des informations sur la date ou la durée et produisant des données de certification de la donnée relative à une date ou une durée destinées à une entité extérieure. Applications notamment aux cartes à microcircuit.

ENTITE ELECTRONIQUE SECURISEE PERMETTANT UNE CERTIFICATION DU TEMPS

L'invention se rapporte à une entité électronique sécurisée permettant une certification du temps. En particulier, à cette fin, la mesure du temps est effectuée dans l'entité électronique sécurisée.

On entend ici une gestion du temps "dans" l'entité électronique au sens où cette gestion est indépendante de tout système extérieur de mesure du temps, qu'il s'agisse par exemple d'un générateur de signal d'horloge ou de tout autre moyen de mesure du temps situé à l'extérieur par rapport à l'entité électronique.

Ces spécificités permettent de rendre relativement inviolable l'entité électronique objet de la présente invention.

L'invention peut s'appliquer à toute entité électronique sécurisée, comme, par exemple, une carte à microcircuit sécurisée.

L'entité électronique sécurisée peut être par exemple une carte à microcircuit sécurisée telle qu'une carte bancaire, une carte de contrôle d'accès, une carte d'identité, une carte SIM (module d'identification de l'abonné, en anglais "*Subscriber Identification Module*") ou une carte mémoire sécurisée (telle qu'une carte SD (Secured Digital) de Panasonic), ou peut être une carte PCMCIA (architecture internationale de cartes-mémoire d'ordinateurs individuels, en anglais "*Personal Computer Memory Card International Architecture*") sécurisée (par exemple, une carte IBM 4758).

Un grand nombre d'applications ont besoin de s'assurer qu'un utilisateur effectue une action dans une période de temps donnée ou avant une date limite.

Par exemple, pour le paiement des impôts à distance, par voie électronique, le contribuable doit se connecter au serveur du Ministère des Finances avant la date limite de paiement de l'impôt et effectuer le paiement en ligne avant cette date. Le serveur s'assure lui-même que le paiement a été effectué dans les délais.

Une telle façon de procéder peut devenir problématique lorsque beaucoup d'utilisateurs ont tendance à réaliser les actions tous au même moment, typiquement juste avant la date limite ou dans la fin de la période autorisée. Le serveur ou les canaux de communication peuvent alors être saturés, à moins de

prévoir, moyennant des coûts élevés, des infrastructures de communication surdimensionnées entre les utilisateurs et le serveur, afin d'absorber les pics de trafic ainsi engendrés.

On pourrait aussi envisager d'utiliser l'heure fournie par l'ordinateur utilisé par le contribuable pour se connecter au serveur du Ministère des Finances. Cependant, l'heure donnée par cet ordinateur pourrait être facilement falsifiée.

La présente invention a pour but de remédier à ces inconvénients, en remplaçant, dans l'exemple précédent, l'heure fournie par l'ordinateur par celle fournie et/ou certifiée par une entité électronique sécurisée. Pour ce faire, la présente invention intègre dans l'entité électronique la mesure du temps.

Dans ce but, l'invention propose une entité électronique sécurisée, remarquable en ce qu'elle contient une unité de mesure du temps et en ce qu'elle comporte une unité de certification d'une donnée relative à une date ou à une durée, l'unité de certification recevant de l'unité de mesure du temps des informations sur la date ou la durée et produisant des données de certification de cette donnée relative à une date ou une durée destinées à une entité extérieure.

L'entité extérieure est typiquement celle où s'exécute une application utilisant l'entité électronique sécurisée pour des besoins de certification de date ou de durée. L'application peut être sous la forme d'un programme informatique exécutable ou sous forme de circuit électronique.

Ainsi, la date est calculée de façon sécurisée, car à l'intérieur de l'entité électronique sécurisée, les tentatives de fraude consistant à falsifier la date sont évitées.

Avantageusement, l'unité de certification est adaptée à fournir une date ou une durée certifiée, ou à certifier l'authenticité d'une date ou d'une durée reçue de l'extérieur, ou encore à certifier qu'une action a été réalisée dans une période de temps donnée ou avant une date limite.

Selon une caractéristique particulière, l'entité électronique sécurisée comporte en outre une unité de synchronisation.

Cela permet de définir une référence de date commune entre l'entité électronique sécurisée et l'application utilisant la date ou la durée à certifier, ou l'action dont la date est à vérifier.

Selon une caractéristique particulière, l'unité de certification met en œuvre des moyens d'authentification, tels que des moyens de chiffrement ou un code d'authentification.

Cela permet de garantir la provenance et l'intégrité des données de certification reçues par l'application en provenance de l'entité électronique sécurisée.

Avantageusement, l'unité de mesure du temps est adaptée à fournir une mesure du temps même lorsque l'entité électronique n'est pas alimentée par une source d'énergie extérieure.

Avantageusement, l'unité de mesure du temps est adaptée à fournir une mesure du temps même lorsque l'entité électronique n'est pas alimentée électriquement.

Avantageusement, l'unité de mesure du temps est adaptée à fournir une mesure du temps indépendamment de tout signal d'horloge extérieur.

En ce sens, l'unité de mesure du temps est autonome, à la fois du point de vue de la mesure du temps et du point de vue de l'alimentation électrique.

En variante, on peut bien entendu prévoir une pile et/ou une horloge dans l'entité électronique.

L'unité de mesure du temps peut comporter un moyen de comparaison de deux dates, une date étant, de façon générale, une expression du temps courant et ces deux dates s'entendant ici comme deux instants définis par rapport à une même référence temporelle.

Dans un mode de réalisation préféré de la présente invention, l'entité électronique sécurisée comporte au moins un sous-ensemble comprenant :

un composant capacitif présentant une fuite au travers de son espace diélectrique, des moyens permettant de coupler ce composant capacitif à une source d'énergie électrique pour être chargé par la source d'énergie électrique et

un moyen de mesure de la charge résiduelle du composant capacitif, cette charge résiduelle étant au moins en partie représentative du temps qui s'est écoulé après que le composant capacitif a été découplé de la source d'énergie électrique.

Dans ce cas, le composant capacitif du sous-ensemble précité ne peut être chargé que lorsque l'entité électronique sécurisée est couplée à la source

d'énergie électrique. Cette dernière peut être extérieure à l'entité électronique sécurisée, mais ce n'est pas impératif : en variante, on peut prévoir d'alimenter l'entité électronique par une pile disposée dans ou sur celle-ci.

L'entité électronique pourra être pourvue d'un moyen de commutation pour découpler le composant capacitif de la source d'énergie électrique, cet événement initialisant la mesure du temps.

Plus généralement, la mesure du temps, c'est-à-dire la variation de charge du composant capacitif, commence dès que, après avoir été chargé, celui-ci se trouve électriquement isolé de tout autre circuit et ne peut plus se décharger qu'à travers son propre espace diélectrique.

Cependant, même si, physiquement, la charge résiduelle mesurée est liée à l'intervalle de temps écoulé entre l'isolement de l'élément capacitif et une mesure donnée de sa charge résiduelle, un intervalle de temps mesuré peut être déterminé entre deux mesures, la première mesure déterminant en quelque sorte une charge résiduelle de référence. Le moyen de mesure de la charge résiduelle du composant capacitif est mis en œuvre lorsqu'on désire connaître un temps écoulé.

Le moyen de mesure de la charge résiduelle peut être compris dans l'unité de mesure du temps mentionnée plus haut.

Dans le mode préféré de réalisation, le moyen de mesure de la charge résiduelle comprend un transistor à effet de champ dont la grille est connectée à une borne du composant capacitif, c'est-à-dire à une "armature" d'une capacité.

Une telle capacité peut être réalisée en technologie MOS et son espace diélectrique peut alors être constitué par un oxyde de silicium. Dans ce cas, il est avantageux que le transistor à effet de champ soit réalisé également en technologie MOS. La grille du transistor à effet de champ et l'"armature" du composant capacitif MOS sont reliées et constituent une sorte de grille flottante qui peut être connectée à un composant permettant d'injecter des porteurs de charge.

On peut aussi faire en sorte qu'il n'existe aucune connexion électrique à proprement parler avec l'environnement extérieur. La connexion de la grille flottante peut être remplacée par une grille de contrôle (électriquement isolée) qui vient charger la grille flottante, par exemple par effet tunnel ou par "porteurs

chauds". Cette grille permet de faire transiter des porteurs de charge vers la grille flottante commune au transistor à effet de champ et au composant capacitif. Cette technique est bien connue des fabricants de mémoires de type EPROM ou EEPROM.

Le transistor à effet de champ et le composant capacitif peuvent constituer une unité intégrée dans un microcircuit compris dans l'entité électronique sécurisée ou faisant partie d'un autre microcircuit logé dans une autre entité sécurisée, telle qu'un serveur.

A certains instants, périodiques ou non, lorsque l'entité électronique sécurisée est couplée à une source d'énergie électrique extérieure, le composant capacitif est chargé à une valeur prédéterminée, connue ou mesurée et mémorisée, et le moyen de mesure de la charge résiduelle est relié à une borne de ce composant capacitif.

Puis le moyen de mesure de la charge résiduelle, notamment le transistor à effet de champ, n'est plus alimenté mais sa grille reliée à la borne du composant capacitif est portée à une tension correspondant à la charge de celui-ci.

Le composant capacitif se décharge lentement au travers de son propre espace diélectrique de sorte que la tension appliquée sur la grille du transistor à effet de champ diminue progressivement.

Lorsqu'une tension électrique est à nouveau appliquée entre le drain et la source du transistor à effet de champ, un courant électrique allant du drain vers la source (ou dans le sens contraire selon les cas) est engendré et peut être recueilli et analysé.

La valeur du courant électrique mesuré dépend des paramètres technologiques du transistor à effet de champ et de la différence de potentiel entre le drain et la source, mais aussi de la tension entre la grille et le substrat. Le courant dépend donc des porteurs de charge accumulés dans la grille flottante commune au transistor à effet de champ et au composant capacitif. Par conséquent, ce courant de drain est aussi représentatif du temps qui s'est écoulé entre une date de référence et la date courante.

Le courant de fuite d'une telle capacité dépend bien sûr de l'épaisseur de son espace diélectrique mais également de tout autre paramètre dit

technologique tel que les longueurs et surfaces de contact des éléments du composant capacitif. Il faut également prendre en compte l'architecture tridimensionnelle des contacts de ces parties, qui peut induire des phénomènes modifiant les paramètres du courant de fuite (par exemple, modification de la valeur de la capacité dite tunnel). Le type et la quantité des dopants et des défauts peuvent être modulés pour modifier les caractéristiques du courant de fuite.

Les variations de température ont aussi une influence, plus précisément la moyenne des apports d'énergie calorifique appliqués à l'entité électronique sécurisée. En fait, tout paramètre intrinsèque à la technologie MOS peut être source de modulation du processus de la mesure du temps.

Avantageusement, l'épaisseur de la couche isolante du transistor à effet de champ est notablement supérieure (par exemple environ trois fois supérieure) à l'épaisseur de la couche isolante du composant capacitif.

Quant à l'épaisseur de la couche isolante du composant capacitif, elle est avantageusement comprise entre 4 et 10 nanomètres.

Pour obtenir une information sensiblement uniquement représentative du temps, on peut prévoir, dans une variante de réalisation, au moins deux sous-ensembles tels que définis ci-dessus, exploités "en parallèle". Les deux composants capacitifs sensibles à la température sont définis avec des fuites différentes, toutes choses égales par ailleurs, c'est-à-dire que leurs espaces diélectriques (épaisseur de la couche d'oxyde de silicium) ont des épaisseurs différentes.

A cet effet, selon une disposition avantageuse de l'invention, l'entité électronique définie ci-dessus est remarquable en ce qu'elle comporte :

au moins deux sous-ensembles précités comprenant chacun :

un composant capacitif présentant une fuite au travers de son espace diélectrique, des moyens permettant de coupler ce composant capacitif à une source d'énergie électrique pour être chargé par cette source d'énergie électrique et

un moyen de mesure de la charge résiduelle du composant capacitif, cette charge résiduelle étant au moins en partie représentative

du temps qui s'est écoulé après que le composant capacitif a été découplé de la source d'énergie électrique,

ces sous-ensembles comprenant des composants capacitifs présentant des fuites différentes au travers de leurs espaces diélectriques respectifs,

et en ce que l'entité électronique sécurisée comporte en outre :

des moyens de traitement des mesures des charges résiduelles respectives de ces composants capacitifs, pour extraire de ces mesures une information sensiblement indépendante des apports calorifiques appliqués à l'entité électronique sécurisée pendant le temps écoulé.

Par exemple, les moyens de traitement peuvent comporter un tableau de valeurs de temps mémorisées, ce tableau étant adressé par ces mesures respectives. Autrement dit, chaque couple de mesures désigne une valeur de temps mémorisée indépendante de la température et des variations de température pendant la période mesurée. L'entité électronique comporte avantageusement une mémoire associée à un microprocesseur et une partie de cette mémoire peut être utilisée pour mémoriser le tableau de valeurs.

En variante, les moyens de traitement peuvent comporter un logiciel de calcul programmé pour exécuter une fonction prédéterminée permettant de calculer l'information temps, sensiblement indépendante des apports calorifiques, en fonction des deux mesures précitées.

Dans un mode particulier de réalisation, l'entité électronique sécurisée est portable. On peut ainsi tirer parti de tous les avantages pratiques de la portabilité, et par exemple transporter dans une poche ou un portefeuille des moyens de certification du temps sans avoir besoin de se connecter à un serveur.

L'invention est particulièrement adaptée à s'appliquer aux cartes à microcircuit. L'entité électronique sécurisée peut être une carte à microcircuit telle qu'une carte bancaire, une carte de contrôle d'accès, une carte d'identité, une carte SIM ou une carte mémoire (telle qu'une carte SD de Panasonic), ou peut comprendre une carte à microcircuit, ou encore peut être d'un autre type, par exemple, être une carte PCMCIA (telle qu'une carte IBM 4758).

L'invention est en outre remarquable par son niveau d'intégration.

D'autres aspects et avantages de l'invention apparaîtront à la lecture de la description détaillée qui suit de modes particuliers de réalisation, donnés à titre d'exemples non limitatifs. La description est faite en référence aux dessins qui l'accompagnent, dans lesquels :

- la figure 1 est un synoptique représentant, dans un mode particulier de réalisation, une entité électronique sécurisée conforme à la présente invention ;
- la figure 2 est un schéma-bloc d'une carte à microcircuit à laquelle peut s'appliquer l'invention, dans un mode particulier de réalisation ;
- la figure 3 est un schéma de principe d'un sous-ensemble que l'entité électronique sécurisée peut comporter dans un mode particulier de réalisation ; et
- la figure 4 est un schéma-bloc d'une variante du mode de réalisation des figures 1 et 2.

Comme le montre la **figure 1**, dans un mode particulier de réalisation, une entité électronique sécurisée 11 conforme à la présente invention contient une unité 18 de mesure du temps.

L'unité 18 ou cellule de mesure du temps est indépendante de tout système extérieur de mesure du temps, qu'il s'agisse par exemple d'un générateur de signal d'horloge ou de tout autre moyen de mesure du temps situé à l'extérieur par rapport à la carte.

L'entité électronique sécurisée 11 comporte en outre une unité 21 de certification, qui reçoit de l'unité 18 de mesure du temps des informations sur le temps écoulé (la date ou une durée).

Conformément à la présente invention, l'unité de certification 21 est adaptée à fournir une date ou une durée certifiée, ou à certifier l'authenticité d'une date ou d'une durée reçue de l'extérieur, ou à certifier qu'une action a été réalisée dans une période de temps donnée ou avant une date limite.

De préférence, l'entité électronique sécurisée 11 comporte une unité 18a de synchronisation, c'est-à-dire des moyens permettant la mise à l'heure de l'unité 18 de mesure du temps. Cette synchronisation peut avoir lieu une seule fois au début de la vie de l'entité électronique, ou bien à un instant donné, ou bien à divers instants.

L'unité 18a de synchronisation peut être constituée par des moyens d'affectation d'une valeur de décalage (en anglais "*offset*") dans un registre, cette valeur de décalage étant ensuite additionnée à la mesure du temps écoulé depuis la charge de l'unité 18 de mesure du temps pour obtenir une date courante.

L'unité 18a de synchronisation peut également lire la cellule de mesure du temps (qui va être décrite ci-après en détail dans un mode particulier de réalisation) en cours de décharge et copier la valeur initiale lue ou la date associée dans un registre, cette valeur initiale étant ensuite soustraite de la mesure du temps écoulé depuis la charge de l'unité 18 de mesure du temps pour obtenir une date courante. Cette synchronisation peut être réalisée par connexion sécurisée à un serveur ou un terminal.

En variante, l'unité 18 de synchronisation peut également réinitialiser la date, par exemple en rechargeant la cellule de mesure du temps.

L'unité 18a de synchronisation peut en outre comporter des moyens adaptés à vérifier l'unicité des messages échangés avec l'application, de façon à éviter qu'un message déjà reçu et copié frauduleusement soit pris en compte une deuxième fois de façon non autorisée. Il peut s'agir typiquement d'un compteur de messages, un numéro étant inséré dans chaque message envoyé à l'application et incrémenté à chaque envoi de message.

L'entité électronique sécurisée 11 peut, par exemple sur requête de l'application utilisant l'entité électronique sécurisée, laquelle est située par exemple sur un terminal associé, collaborer avec l'application pour certifier qu'un utilisateur effectue une action dans une période de temps donnée ou avant une date limite.

Sur requête de l'application, l'entité électronique sécurisée 11 peut ainsi :

- fournir une date ou une durée certifiée : typiquement, la date retournée par l'entité électronique est accompagnée d'un code d'authentification de la date (obtenu par une technique connue de l'homme du métier, en utilisant par exemple une fonction de hachage telle que SHA-1 ou MD-5, et un algorithme de signature tel que l'algorithme RSA). La date et le code d'authentification sont retournés sous forme cryptée afin de garantir la sécurité de la communication,

- valider une date ou une durée donnée par l'application : typiquement, après avoir vérifié la vraisemblance de la date ou de la durée donnée par l'application en utilisant les données reçues de l'unité 18 de mesure du temps, l'entité électronique sécurisée 11 retourne un code d'authentification de la date reçue (obtenu par une technique connue de l'homme du métier, en utilisant par exemple une fonction de hachage telle que SHA-1 ou MD-5, et un algorithme de signature tel que l'algorithme RSA),

- certifier qu'une action a été réalisée dans une période de temps donnée ou avant une date limite : typiquement, l'entité électronique retourne, éventuellement ultérieurement, un code d'authentification de la date et des données représentatives de l'action (ce code étant obtenu par une technique connue de l'homme du métier, en utilisant par exemple une fonction de hachage telle que SHA-1 ou MD-5, et un algorithme de signature tel que l'algorithme RSA). Les données représentatives de l'action et le code d'authentification sont retournés sous forme cryptée afin de garantir la sécurité de la communication. L'entité électronique reçoit par exemple directement les données représentatives de l'action en provenance de l'application. Dans le mode particulier de réalisation où l'entité électronique est une carte à microcircuit, ces données représentatives peuvent être envoyées par l'application et communiquées à la carte sous forme de commandes du type APDU. En variante, l'entité électronique peut reconnaître elle-même l'action et calculer les données représentatives de cette action.

On décrit maintenant, à titre d'exemples nullement limitatifs, trois applications possibles de la présente invention.

Dans le domaine des courses hippiques, considérons un joueur qui s'inscrit avec son téléphone portable en début de journée auprès du serveur d'un hippodrome. La carte SIM associée au téléphone portable reçoit sous forme chiffrée une heure de référence et un code d'authentification de cette heure de référence (permettant à la carte de vérifier que l'heure de référence est bien fournie par le serveur de l'hippodrome). La carte SIM déchiffre l'heure et l'associe à l'état de la charge de la cellule de mesure du temps. L'heure et la charge sont inscrites dans un fichier en EEPROM. On procède ainsi à la synchronisation de la carte SIM et du serveur de l'hippodrome. Le joueur précise aussi au serveur la somme maximale qu'il souhaite jouer (cette somme sera

débitée du compte du joueur si celui-ci ne se reconnecte pas au réseau dans les jours qui viennent) et cette somme est aussi écrite dans le fichier en EEPROM.

Plus tard dans la journée, le joueur parie au moyen de son téléphone portable en indiquant le numéro de la course, le numéro du cheval ainsi que la somme qu'il souhaite parier. La carte SIM soustrait alors la somme inscrite dans le fichier en EEPROM du montant du pari. Dès que le crédit restant au joueur devient négatif ou nul, la carte SIM refuse de prendre en compte le pari. La carte SIM mémorise également les données du pari, par exemple un ordre d'arrivée de chevaux anticipé par le joueur.

Ensuite, la carte SIM détermine l'heure du pari en comparant la charge actuelle de la cellule avec la charge de référence et l'heure inscrites dans le fichier en EEPROM.

Cette heure, ainsi que les données du pari, sont chiffrées puis sont envoyées au serveur de l'hippodrome par la carte SIM, éventuellement après l'heure limite de fin de jeu de la course considérée, c'est-à-dire après la clôture des paris. La carte SIM envoie également un code d'authentification de l'heure et des données du pari. Pour des raisons de sécurité, le code d'authentification est également envoyé sous forme chiffrée.

Le serveur reçoit ces informations et déchiffre les données du pari et l'heure à laquelle a été effectué le pari. Le serveur vérifie également le code d'authentification reçu afin de s'assurer que ces informations ont bien été envoyées par la carte, et non de façon frauduleuse. Si l'heure déchiffrée indique que le pari a été fait avant la clôture des paris pour la course considérée, le serveur valide le pari ; sinon, il le rejette.

Ainsi, en vertu de la présente invention, le joueur n'est pas obligé d'être physiquement présent à l'hippodrome et/ou d'être relié au serveur durant le pari. Par exemple, au moment du pari, le téléphone du joueur peut se trouver dans une région non couverte par le réseau de téléphonie mobile, ou bien le serveur peut être saturé. Cela n'empêchera pas le joueur de faire valider son pari, car la carte SIM conservera en EEPROM les informations relatives au pari et dès que le téléphone reviendra dans la zone de couverture du réseau, ou dès que le serveur sera à nouveau disponible, la carte SIM enverra au serveur les données relatives au pari.

Dans le domaine des élections faites par téléphone portable, par exemple dans le cadre de certaines émissions télévisées, à un moment donné, un électeur reçoit sur son téléphone un message lui indiquant qu'il peut voter et ce, jusqu'à une certaine date limite. Avec ce message, la date et l'heure courante sont aussi transmises, sous forme chiffrée. La carte SIM du téléphone portable reçoit ce message et déchiffre la date. Elle associe alors la charge de la cellule avec cette date et écrit ces deux données dans un fichier en EEPROM. La synchronisation avec l'entité ayant fourni le message est ainsi réalisée.

Au moment du vote, la carte SIM associe la charge courante de la cellule de mesure du temps avec une date en fonction de la charge et de la date de référence contenues dans le fichier en EEPROM. Cette date, le choix de l'électeur, ainsi qu'un code d'authentification de cette date et de ce choix, sont chiffrés puis envoyés au serveur.

A réception, le serveur déchiffre la date et le choix de l'électeur, vérifie le code d'authentification, puis accepte ou refuse le vote suivant la valeur de la date.

De même que dans l'exemple précédent, le vote peut être effectué sans que le téléphone de l'électeur soit immédiatement connecté au serveur, mémorisé, puis transmis au serveur quelques jours plus tard.

Dans le domaine des logiciels à durée d'utilisation limitée, au début de l'utilisation du logiciel, une carte à microcircuit, associée à l'ordinateur sur lequel on fait fonctionner le logiciel, recharge la cellule de mesure du temps.

Ensuite, à tout instant au cours de l'utilisation du logiciel, la carte peut lire la charge courante de la cellule de mesure du temps, pour obtenir la durée d'utilisation actuelle du logiciel. Par exemple sur demande du logiciel, la carte renvoie cette durée au logiciel accompagnée d'un code d'authentification, le tout sous forme chiffrée. Le logiciel déchiffre la durée reçue et vérifie le code d'authentification reçu afin de s'assurer que ces données sont bien fournies par la carte. Si cette durée d'utilisation est inférieure à la durée autorisée alors le logiciel continue de fonctionner normalement ; sinon, le logiciel ne peut plus fonctionner.

Le logiciel peut aussi demander à la carte de valider la date fournie par le terminal sur lequel le logiciel fonctionne. Par exemple, la carte peut vérifier que

la date fournie par le terminal est celle mesurée par la carte à ± 24 heures près, si la licence d'utilisation du logiciel est concédée par exemple pour une durée d'un an. Ainsi, la carte à microcircuit n'a pas besoin de mesurer le temps avec une très grande précision.

Il est à noter qu'il existe beaucoup de variantes dans l'utilisation de la cellule de mesure du temps : on peut utiliser une cellule chargée au début de la vie de la carte, ou une cellule qui se recharge au moment de la synchronisation (par exemple, lors de l'inscription au serveur de l'hippodrome dans l'exemple des courses hippiques, lors de la réception du message indiquant la possibilité de voter dans l'exemple des votes électroniques, ou au début de l'utilisation du logiciel dans l'exemple des logiciels à durée d'utilisation limitée). Dans l'exemple des logiciels à durée d'utilisation limitée, au cas où on considère plusieurs logiciels, on peut utiliser plusieurs cellules de mesure du temps, chacune étant dédiée à un logiciel spécifique.

La **figure 2** illustre une entité électronique sécurisée 11 conforme à la présente invention, dans un mode particulier de réalisation où cette entité est une carte à microcircuit. L'entité électronique sécurisée 11 comporte une unité 12 lui permettant d'être couplée à une source d'énergie électrique extérieure 16.

Dans le mode particulier de réalisation représenté, l'entité électronique sécurisée 11 comporte des plages de raccordement métalliques susceptibles d'être connectées à une unité formant un lecteur de carte. Deux de ces plages de raccordement 13a, 13b sont réservées à l'alimentation électrique du microcircuit, la source d'énergie électrique étant logée dans un serveur ou autre dispositif auquel l'entité électronique sécurisée est momentanément raccordée. Ces plages de raccordement peuvent être remplacées par une antenne logée dans l'épaisseur de la carte et susceptible de fournir au microcircuit l'énergie électrique nécessaire à son alimentation tout en assurant la transmission bidirectionnelle de signaux radiofréquence permettant les échanges d'informations. On parle alors de technologie sans contact.

Le microcircuit comprend un microprocesseur 14 associé de façon classique à une mémoire 15.

Dans un exemple particulier de réalisation, l'entité électronique sécurisée 11 comporte au moins un sous-ensemble 17 (ou est associée à un tel sous-ensemble) chargé de la mesure du temps.

Le sous-ensemble 17, qui est représenté plus en détail sur la **figure 3**, est donc logé dans l'entité électronique sécurisée 11. Il peut faire partie du microcircuit et être réalisé dans la même technologie d'intégration que celui-ci.

Le sous-ensemble 17 comprend un composant capacitif 20 présentant une fuite au travers de son espace diélectrique 24 et une unité 22 de mesure de la charge résiduelle de ce composant 20.

Cette charge résiduelle est au moins en partie représentative du temps écoulé après que le composant capacitif 20 a été découplé de la source d'énergie électrique.

Le composant capacitif 20 est chargé par la source d'énergie électrique extérieure soit par connexion directe, comme dans l'exemple décrit, soit par tout autre moyen qui peut amener à charger la grille. L'effet tunnel est une méthode permettant de charger la grille sans connexion directe. Dans l'exemple, la charge du composant capacitif 20 est pilotée par le microprocesseur 14.

Dans l'exemple, le composant capacitif 20 est une capacité réalisée suivant la technologie MOS. L'espace diélectrique 24 de cette capacité est constitué par une couche d'oxyde de silicium déposée à la surface d'un substrat 26 constituant une des armatures du condensateur. Ce substrat 26 est ici connecté à la masse, c'est-à-dire à une des bornes d'alimentation de la source d'énergie électrique extérieure, lorsque celle-ci se trouve raccordée à la carte. L'autre armature du condensateur est un dépôt conducteur 28a appliqué sur l'autre face de la couche d'oxyde de silicium.

Par ailleurs, l'unité 22 de mesure mentionnée précédemment comprend essentiellement un transistor 30 à effet de champ, ici réalisé suivant la technologie MOS, comme la capacité. La grille du transistor 30 est connectée à une borne du composant capacitif 20. Dans l'exemple, la grille est un dépôt conducteur 28b de même nature que le dépôt conducteur 28a qui, comme indiqué ci-dessus, constitue une des armatures du composant capacitif 20.

Les deux dépôts conducteurs 28a et 28b sont reliés l'un à l'autre ou ne constituent qu'un seul et même dépôt conducteur. Une connexion 32 reliée au

microprocesseur 14 permet d'appliquer une tension à ces deux dépôts 28a et 28b, pendant un court intervalle de temps nécessaire pour charger le composant capacitif 20. L'application de cette tension est pilotée par le microprocesseur 14.

Plus généralement, la connexion 32 permet de charger le composant capacitif 20 à un moment choisi, sous la commande du microprocesseur 14 et c'est à partir du moment où cette connexion de charge est coupée par le microprocesseur 14 (ou lorsque l'entité électronique sécurisée 11 est découplée dans son ensemble de toute source d'alimentation électrique) que la décharge du composant capacitif 20 au travers de son espace diélectrique 24 commence, cette perte de charge électrique étant représentative du temps écoulé. La mesure du temps implique la mise en conduction momentanée du transistor 30, ce qui suppose la présence d'une source d'énergie électrique appliquée entre drain et source.

Le transistor 30 à effet de champ en technologie MOS comporte, outre la grille, un espace diélectrique de grille 34 séparant cette dernière d'un substrat 36 dans lequel sont définies une région de drain 38 et une région de source 39. L'espace diélectrique de grille 34 est constitué par une couche isolante d'oxyde de silicium. La connexion de source 40 appliquée à la région de source 39 est reliée à la masse et au substrat 36. La connexion de drain 41 est reliée à un circuit de mesure du courant de drain qui comporte une résistance 45 aux bornes de laquelle sont connectées les deux entrées d'un amplificateur différentiel 46. La tension délivrée à la sortie de cet amplificateur est donc proportionnelle au courant de drain.

La grille 28b est mise en position flottante pendant qu'on mesure le temps écoulé. Autrement dit, aucune tension n'est appliquée à la grille pendant cette même mesure. En revanche, puisque la grille est connectée à une armature du composant capacitif 20, la tension de grille pendant cette même mesure est égale à une tension qui se développe entre les bornes du composant capacitif 20 et qui résulte d'une charge initiale de celui-ci réalisée sous le contrôle du microprocesseur 14.

L'épaisseur de la couche isolante du transistor 30 est notablement plus grande que celle du composant capacitif 20. A titre d'exemple non limitatif, l'épaisseur de la couche isolante du transistor 30 peut être environ trois fois

supérieure à l'épaisseur de la couche isolante du composant capacitif 20. Selon l'application envisagée, l'épaisseur de la couche isolante du composant capacitif 20 est comprise entre 4 et 10 nanomètres, environ.

Lorsque le composant capacitif 20 est chargé par la source d'énergie électrique extérieure et après que la connexion de charge a été coupée sous la commande du microprocesseur 14, la tension aux bornes du composant capacitif 20 diminue lentement au fur et à mesure que ce dernier se décharge progressivement au travers de son propre espace diélectrique 24. La décharge au travers de l'espace diélectrique 34 du transistor 30 à effet de champ est négligeable compte tenu de l'épaisseur de ce dernier.

A titre d'exemple nullement limitatif, si, pour une épaisseur d'espace diélectrique donnée, on charge la grille et l'armature du composant capacitif 20 à 6 volts à un instant t = 0, le temps associé à une perte de charge de 1 volt, c'est-à-dire un abaissement de la tension à une valeur de 5 volts, est de l'ordre de 24 secondes pour une épaisseur de 8 nanomètres.

Pour des épaisseurs différentes, on peut dresser le tableau suivant :

Durée	1 heure	1 journée	1 semaine	1 mois
Epaisseur d'oxyde	8,17 nm	8,79 nm	9,17 nm	9,43 nm
Précision sur le temps	1,85 %	2,09 %	2,24 %	3,10 %

La précision dépend de l'erreur commise sur la lecture du courant de drain (0,1 % environ). Ainsi, pour pouvoir mesurer des temps de l'ordre d'une semaine, on peut prévoir une couche d'espace diélectrique de l'ordre de 9 nanomètres.

La figure 3 montre une architecture particulière qui utilise une connexion directe à la grille flottante (28a, 28b) pour y appliquer un potentiel électrique et donc y faire transiter des charges. On peut aussi procéder à une charge indirecte, comme mentionné précédemment, grâce à une grille de contrôle remplaçant la connexion directe, selon la technologie utilisée pour la fabrication des cellules EPROM ou EEPROM.

La variante de la **figure 4** prévoit trois sous-ensembles 17A, 17B, 17C, chacun associé au microprocesseur 14. Les sous-ensembles 17A et 17B

comprennent des composants capacitifs présentant des fuites relativement faibles pour permettre des mesures de temps relativement longs.

Cependant, ces composants capacitifs sont généralement sensibles aux variations de température. Le troisième sous-ensemble 17C comporte un composant capacitif présentant un espace diélectrique très faible, inférieur à 5 nanomètres. Il est de ce fait insensible aux variations de température. Les deux composants capacitifs des sous-ensembles 17A, 17B présentent des fuites différentes au travers de leurs espaces diélectriques respectifs.

En outre, l'entité électronique sécurisée comporte un module de traitement des mesures des charges résiduelles respectives présentes dans les composants capacitifs des deux premiers sous-ensembles 17A, 17B. Ce module de traitement est adapté à extraire de ces mesures une information représentative des temps et sensiblement indépendante des apports calorifiques appliqués à l'entité électronique sécurisée pendant le temps écoulé.

Dans l'exemple, ce module de traitement se confond avec le microprocesseur 14 et la mémoire 15. En particulier, un espace de la mémoire 15 est réservé à la mémorisation d'un tableau T à double entrée de valeurs de temps et ce tableau est adressé par les deux mesures respectives issues des sous-ensembles 17A et 17B. Autrement dit, une partie de la mémoire comporte un ensemble de valeurs de temps et chaque valeur correspond à un couple de mesures résultant de la lecture du courant de drain de chacun des deux transistors des sous-ensembles 17A, 17B sensibles à la température.

Ainsi, au début d'une opération de mesure du temps écoulé, les deux composants capacitifs sont chargés, à une valeur de tension prédéterminée, par la source d'énergie électrique extérieure, via le microprocesseur 14. Lorsque la carte à microcircuit est découplée du serveur ou lecteur de carte ou autre entité, les deux composants capacitifs restent chargés mais commencent à se décharger au travers de leurs propres espaces diélectriques respectifs et, au fur et à mesure que le temps s'écoule, sans que la carte à microcircuit soit utilisée, la charge résiduelle de chacun des composants capacitifs décroît mais différemment dans l'un ou l'autre, en raison des fuites différentes déterminées par construction.

Lorsque la carte est à nouveau couplée à une source d'énergie électrique extérieure, les charges résiduelles des deux composants capacitifs sont représentatives du même intervalle de temps qu'on cherche à déterminer mais diffèrent en raison des variations de température qui ont pu se produire pendant toute cette période de temps.

Pour chaque couple de valeurs de courant de drain, le microcircuit va chercher en mémoire, dans le tableau T mentionné précédemment, la valeur de temps correspondante.

Il n'est pas nécessaire de mémoriser le tableau T. Par exemple, le module de traitement, c'est-à-dire essentiellement le microprocesseur 14, peut comporter une partie de logiciel de calcul d'une fonction prédéterminée permettant de déterminer ladite information sensiblement indépendante des apports calorifiques en fonction des deux mesures.

Le troisième sous-ensemble 17C comporte, comme décrit plus haut, un espace diélectrique extrêmement mince le rendant insensible aux variations de température.

D'autres variantes sont possibles. En particulier, si on veut simplifier le sous-ensemble 17, on peut envisager de supprimer le composant capacitif 20 en tant que tel, car le transistor 30 à effet de champ peut lui-même être considéré comme un composant capacitif avec la grille 28b et le substrat 36 en tant qu'armatures, ces dernières étant séparées par l'espace diélectrique 34. Dans ce cas, on peut considérer que le composant capacitif et l'unité de mesure sont confondus.

On peut mesurer le temps ou une durée écoulé depuis une date de référence, par exemple la date de la synchronisation, de diverses façons.

Une première possibilité consiste à charger la cellule qui mesure le temps une fois, lors de la première mise en service de l'entité électronique. A chaque instant, l'état de la charge de la cellule de mesure du temps est représentatif du temps écoulé depuis la première mise en service.

Une deuxième possibilité consiste à recharger la cellule à chaque mise sous tension de l'entité électronique sécurisée. On mesure ainsi des temps plus courts, qu'on vient cumuler : à chaque mise sous tension, le temps écoulé depuis la dernière mise sous tension de l'entité électronique sécurisée est

mesuré, puis le composant capacitif est rechargé. On accumule les temps ainsi mesurés dans un emplacement de la mémoire non volatile de l'entité électronique.

Cet emplacement mémoire mémorise ainsi le temps écoulé depuis la première mise sous tension et permet de connaître à tout moment le temps écoulé.

Le temps qui s'écoule entre l'instant de mesure de la charge du composant capacitif et le moment de sa recharge est parfois non négligeable. Pour prendre en compte cet intervalle de temps, on peut utiliser un second composant dont la fonction sera de prendre le relais du premier pendant cet intervalle de temps.

On peut également utiliser une cellule par besoin de validation ou de certification. Dans ce cas, on rechargera de préférence chaque cellule lors de la synchronisation.

On peut également prévoir d'utiliser des composants capacitifs de précisions différentes afin d'améliorer la précision de la mesure : on choisira, parmi plusieurs mesures, celle obtenue à partir du composant le plus précis qui n'est pas déchargé.

D'autres variantes, à la portée de l'homme du métier, sont possibles.

Ainsi, conformément à l'invention, l'utilisation du compteur de temps à l'intérieur de la carte permet d'améliorer la sécurité puisque le décompte du temps est difficile à falsifier.

L'entité électronique sécurisée conforme à la présente invention peut coopérer avec une ou plusieurs autres entités sécurisées qui, en fonction du résultat de la certification, concéderont ou non des droits à un utilisateur, par exemple.

REVENDICATIONS

1. Entité électronique sécurisée (11), caractérisée en ce qu'elle contient un moyen (18) de mesure du temps et en ce qu'elle comporte un moyen (21) de certification d'une donnée relative à une date ou une durée, ledit moyen (21) de certification recevant dudit moyen (18) de mesure du temps des informations sur ladite date ou ladite durée et produisant des données de certification de ladite donnée relative à une date ou une durée destinées à une entité extérieure.

2. Entité électronique sécurisée (11) selon la revendication 1, caractérisée en ce que ledit moyen (21) de certification est adapté à fournir une date ou une durée certifiée.

3. Entité électronique sécurisée (11) selon la revendication 1, caractérisée en ce que ledit moyen (21) de certification est adapté à certifier l'authenticité d'une date ou d'une durée reçue de l'extérieur.

4. Entité électronique sécurisée (11) selon la revendication 1 ou 2, caractérisée en ce que ledit moyen (21) de certification est adapté à certifier qu'une action a été réalisée dans une période de temps donnée ou avant une date limite.

5. Entité électronique sécurisée (11) selon l'une quelconque des revendications précédentes, caractérisée en ce qu'elle comporte en outre des moyens (18a) de synchronisation.

6. Entité électronique sécurisée (11) selon l'une quelconque des revendications précédentes, caractérisée en ce que ledit moyen (21) de certification met en œuvre des moyens d'authentification.

7. Entité électronique sécurisée (11) selon l'une quelconque des revendications précédentes, caractérisée en ce que le moyen (18) de mesure du temps est adapté à fournir une mesure du temps lorsque l'entité électronique (11) n'est pas alimentée par une source d'énergie extérieure.

8. Entité électronique sécurisée (11) selon l'une quelconque des revendications précédentes, caractérisée en ce que le moyen (18) de mesure du temps est adapté à fournir une mesure du temps lorsque l'entité électronique (11) n'est pas alimentée électriquement.

9. Entité électronique sécurisée (11) selon l'une quelconque des revendications précédentes, caractérisée en ce que le moyen (18) de mesure du temps est adapté à fournir une mesure du temps indépendamment de tout signal d'horloge extérieur.

10. Entité électronique sécurisée (11) selon l'une quelconque des revendications précédentes, caractérisée en ce que le moyen (18) de mesure du temps comporte un moyen de comparaison de deux dates.

11. Entité électronique sécurisée (11) selon l'une quelconque des revendications précédentes, caractérisée en ce qu'elle comporte au moins un sous-ensemble (17) comprenant :

un composant capacitif (20) présentant une fuite au travers de son espace diélectrique, des moyens permettant de coupler ledit composant capacitif à une source d'énergie électrique pour être chargé par ladite source d'énergie électrique et

un moyen (22) de mesure de la charge résiduelle du composant capacitif (20), ladite charge résiduelle étant au moins en partie représentative du temps qui s'est écoulé après que le composant capacitif (20) a été découplé de la source d'énergie électrique.

12. Entité électronique sécurisée (11) selon la revendication précédente, caractérisée en ce que ledit moyen (22) de mesure de la charge résiduelle est compris dans ledit moyen (18) de mesure du temps.

13. Entité électronique sécurisée (11) selon la revendication 11 ou 12, caractérisée en ce que le composant capacitif (20) est une capacité réalisée suivant la technologie MOS et dont l'espace diélectrique est constitué par un oxyde de silicium.

14. Entité électronique sécurisée (11) selon la revendication 11, 12 ou 13, caractérisée en ce que le moyen (22) de mesure de la charge résiduelle comprend un transistor (30) à effet de champ ayant une couche isolante (34), en ce que le composant capacitif (20) comporte une couche isolante (24) et en ce que l'épaisseur de la couche isolante (34) du transistor (30) à effet de champ est notablement plus grande que l'épaisseur de la couche isolante (24) du composant capacitif (20).

15. Entité électronique sécurisée (11) selon la revendication précédente, caractérisée en ce que l'épaisseur de la couche isolante (24) du composant capacitif (20) est comprise entre 4 et 10 nanomètres.

16. Entité électronique sécurisée (11) selon la revendication 13, 14 ou 15, caractérisée en ce qu'elle comporte :

au moins deux sous-ensembles (17A, 17B) comprenant chacun :

un composant capacitif présentant une fuite au travers de son espace diélectrique, des moyens permettant de coupler ledit composant capacitif à une source d'énergie électrique pour être chargé par ladite source d'énergie électrique et

un moyen de mesure de la charge résiduelle du composant capacitif, ladite charge résiduelle étant au moins en partie représentative du temps qui s'est écoulé après que le composant capacitif a été découplé de la source d'énergie électrique,

lesdits sous-ensembles (17A, 17B) comprenant des composants capacitifs présentant des fuites différentes au travers de leurs espaces diélectriques respectifs,

et en ce que ladite entité électronique sécurisée (11) comporte en outre :

des moyens (14, 15, T) de traitement des mesures des charges résiduelles respectives desdits composants capacitifs, pour extraire desdites mesures une information sensiblement indépendante des apports calorifiques appliqués à ladite entité (11) pendant le temps écoulé.

17. Entité électronique sécurisée (11) selon la revendication précédente, caractérisée en ce que lesdits moyens (14, 15, T) de traitement comportent un logiciel de calcul d'une fonction prédéterminée pour déterminer ladite information sensiblement indépendante des apports calorifiques en fonction desdites mesures.

18. Entité électronique sécurisée selon l'une quelconque des revendications précédentes, caractérisée en ce qu'elle est portable.

19. Entité électronique sécurisée (11) selon l'une quelconque des revendications précédentes, caractérisée en ce qu'il s'agit d'une carte à microcircuit.

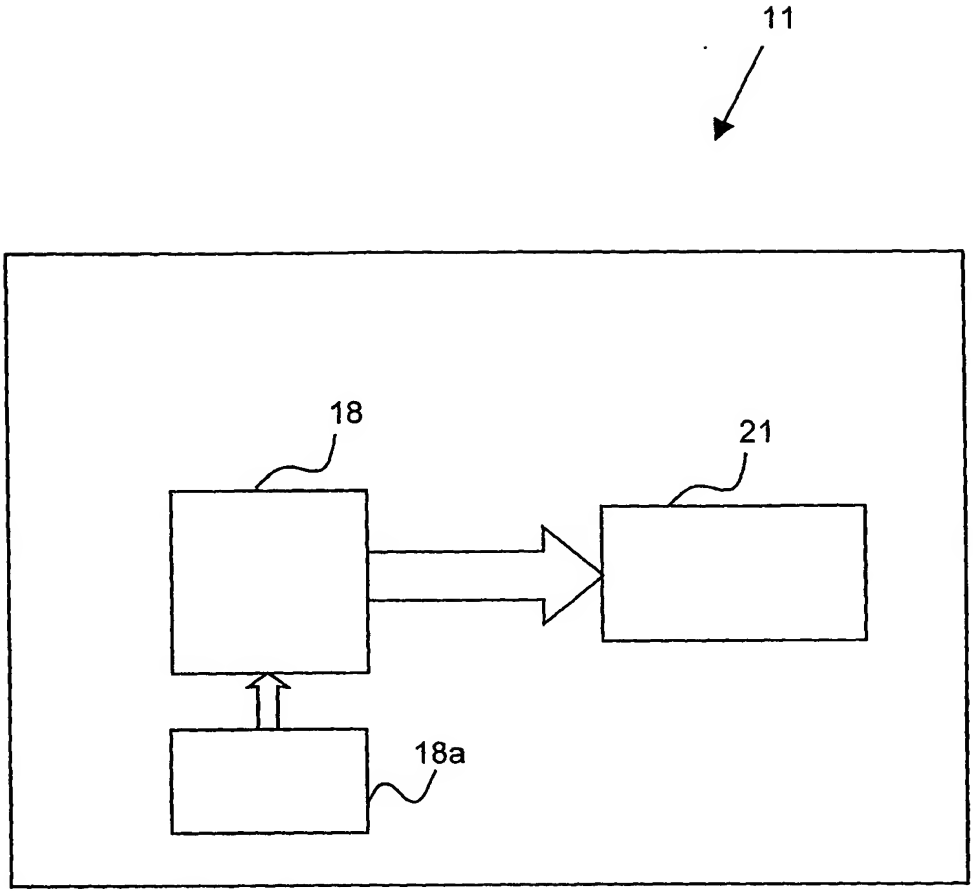


FIG. 1

Fig.2

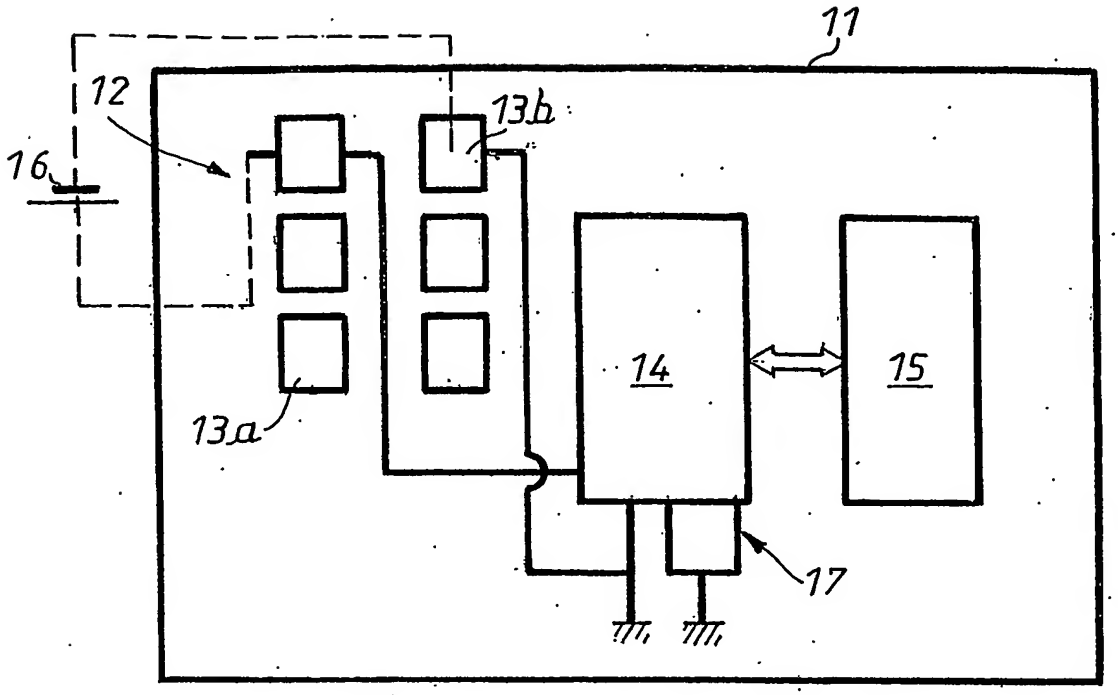


Fig.3

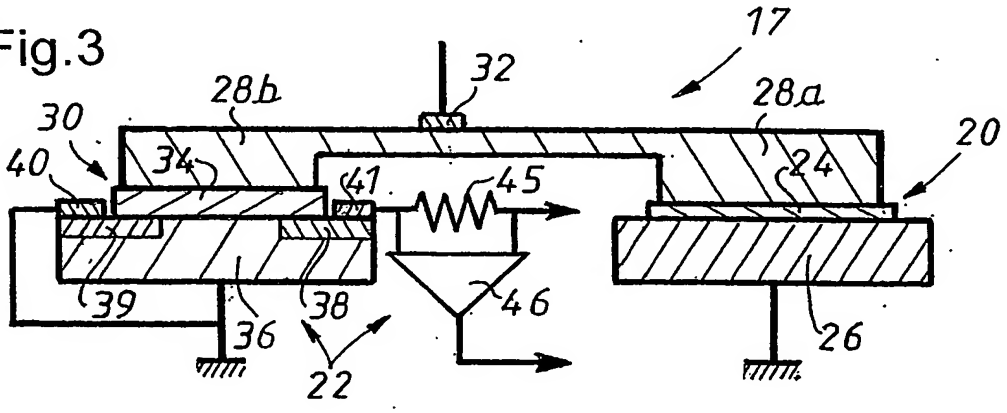
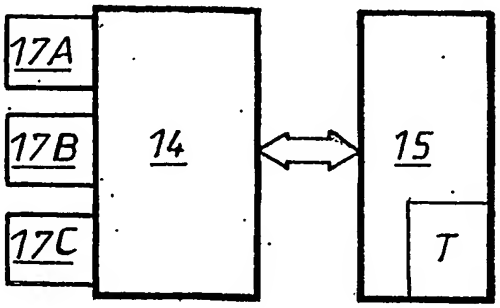


Fig.4



INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR [redacted]/03657

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06K19/073

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G07C G06K

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, PAJ, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	FR 2 764 977 A (STELLA) 24 December 1998 (1998-12-24) page 7, line 14 - line 20 page 8, line 9 - line 23 page 9, line 14 - line 32	1,2,4,6, 7,9,18, 19
Y	---	11-13
Y	WO 01 54057 A (HORVAT HELMUT ;WALLSTAB STEFAN (DE); INFINEON TECHNOLOGIES AG (DE)) 26 July 2001 (2001-07-26) page 4, line 19 -page 5, line 15 page 9, line 11 -page 11, line 30	11-13
A	---	14-16
	-/--	

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
6 April 2004	23/04/2004

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Bhalodia, A

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

Int[redacted]nal Application No
PCT/[redacted]3/03657

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 1 160 736 A (TENOVIS GMBH & CO KG) 5 December 2001 (2001-12-05) column 1, line 9 - line 26 column 4, line 22 -column 5, line 23 ---	1,2,9
A	EP 0 257 648 A (TOKYO SHIBAURA ELECTRIC CO) 2 March 1988 (1988-03-02) column 5, line 25 - line 41 column 10, line 17 - line 45 column 13, line 55 -column 14, line 18 -----	1

INTERNATIONAL SEARCH REPORT

Inte onal Application No
PCT/F /03657

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
FR 2764977 A	24-12-1998	FR 2764977 A1	24-12-1998
		CN 1260872 T	19-07-2000
		EP 0988511 A1	29-03-2000
		WO 9858238 A1	23-12-1998
		US 2002047781 A1	25-04-2002
WO 0154057 A	26-07-2001	WO 0154057 A1	26-07-2001
		EP 1249003 A1	16-10-2002
		US 2003005315 A1	02-01-2003
EP 1160736 A	05-12-2001	DE 10027005 A1	03-01-2002
		EP 1160736 A2	05-12-2001
EP 0257648 A	02-03-1988	JP 2597553 B2	09-04-1997
		JP 63058566 A	14-03-1988
		JP 7046294 B	17-05-1995
		JP 63058524 A	14-03-1988
		DE 3780381 D1	20-08-1992
		DE 3780381 T2	25-02-1993
		EP 0257648 A2	02-03-1988
		KR 9101263 B1	26-02-1991
		US 4766294 A	23-08-1988

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No
PCT/FR[redacted]/03657

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 G06K19/073

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 G07C G06K

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
EPO-Internal, PAJ, WPI Data

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	FR 2 764 977 A (STELLA) 24 décembre 1998 (1998-12-24) page 7, ligne 14 - ligne 20 page 8, ligne 9 - ligne 23 page 9, ligne 14 - ligne 32	1,2,4,6, 7,9,18, 19
Y	---	11-13
Y	WO 01 54057 A (HORVAT HELMUT ;WALLSTAB STEFAN (DE); INFINEON TECHNOLOGIES AG (DE)) 26 juillet 2001 (2001-07-26) page 4, ligne 19 -page 5, ligne 15 page 9, ligne 11 -page 11, ligne 30	11-13
A	---	14-16
	-/--	

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent
"E" document antérieur, mais publié à la date de dépôt international ou après cette date
"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)
"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens
"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée
"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention
"X" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément
"Y" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier
"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
6 avril 2004	23/04/2004

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Bhalodia, A

Formulaire PCT/ISA/210 (deuxième feuille) (Janvier 2004)

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	EP 1 160 736 A (TENOVIS GMBH & CO KG) 5 décembre 2001 (2001-12-05) colonne 1, ligne 9 - ligne 26 colonne 4, ligne 22 -colonne 5, ligne 23	1,2,9
A	EP 0 257 648 A (TOKYO SHIBAURA ELECTRIC CO) 2 mars 1988 (1988-03-02) colonne 5, ligne 25 - ligne 41 colonne 10, ligne 17 - ligne 45 colonne 13, ligne 55 -colonne 14, ligne 18	1

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No
PCT/[redacted]3/03657

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
FR 2764977	A	24-12-1998	FR	2764977 A1	24-12-1998
			CN	1260872 T	19-07-2000
			EP	0988511 A1	29-03-2000
			WO	9858238 A1	23-12-1998
			US	2002047781 A1	25-04-2002
WO 0154057	A	26-07-2001	WO	0154057 A1	26-07-2001
			EP	1249003 A1	16-10-2002
			US	2003005315 A1	02-01-2003
EP 1160736	A	05-12-2001	DE	10027005 A1	03-01-2002
			EP	1160736 A2	05-12-2001
EP 0257648	A	02-03-1988	JP	2597553 B2	09-04-1997
			JP	63058566 A	14-03-1988
			JP	7046294 B	17-05-1995
			JP	63058524 A	14-03-1988
			DE	3780381 D1	20-08-1992
			DE	3780381 T2	25-02-1993
			EP	0257648 A2	02-03-1988
			KR	9101263 B1	26-02-1991
			US	4766294 A	23-08-1988